http://www.palomine.net/qmail/relaying.html

The Qmail Newbie's Guide To Relaying

Courtsey to Chris Johnson

Answer to ::

'Sorry, that domain isn't in my list of allowed rcpthosts'

What exactly is relaying, anyway?
You've set up your qmail server. It's hosting a few domains (i.e. they're listed in your locals file or your virtualdomains file). You've set things up so that qmail-smtpd can take connections on port 25 to receive mail from other hosts.

Another host on the Internet connects to your server on port 25. This might be another mail server running qmail, sendmail, or some other mail transfer agent, or it might be an end user, who wants to send mail from his desktop mail client. The SMTP conversation starts off with the remote host identifying itself:

HELO somehost.somewhere.net
Your server responds:

250 mail.yourdomain.net
The remote host sends the "From" part of the envelope:

MAIL FROM:
Your host responds with:

250 ok
The remote host now sends one or more RCPT TO commands, which specify the recipients of the message:

RCPT TO:
Just a minute! elsewhere.com is not one of the domains that your server hosts. What does your server do? It can agree to accept the message and attempt to deliver it:

250 ok
Or it can reject it:

553 sorry, that domain isn't in my list of allowed rcpthosts (#5.7.1)
In the first case, your server is acting as a relay: it's accepting and agreeing to try to deliver a message that's not destined for a domain that your server hosts. In the second case, it's refusing to act as a relay.

qmail's rcpthosts file, which gets its name from the RCPT TO command, determines whether the recipient will be accepted: it will be accepted if and only if the domain of the address given in the RCPT TO command is listed in rcpthosts. (I'll talk about exceptions to this rule later on.) If the rcpthosts file does not exist, then any recipient will be accepted.

An SMTP server is an "open relay" if it agrees to relay mail no matter who's sending it–if another host connects to port 25 with some mail, an open relay will accept and try to deliver it no matter

what its destination is and no matter who is sending it. A qmail server without a rcpthosts file will act as an open relay.

So why shouldn't I have an open relay? My customers need to send mail to other domains. And why would anyone but my customers want to use my server as a relay, anyway?

This was a safe attitude several years ago; people generally used the relay provided by their ISP, employer, or university.

Then came the spammers, the mass-mailers of unsolicited commercial e-mail. Rather than use their own bandwidth and server resources, they seek open relays that will accept a single message with, say, 100,000 recipients, and distribute it for them. This consumes the bandwidth and server resources of an unwitting third party, and the administrators of the relaying server will likely be flooded with complaints from the spam's recipients. The relaying server may even find itself blacklisted, so that other hosts on the Internet will refuse to receive mail from it (see http://www.ordb.org, for example). Leaving your mail relay open these days is considered to be irresponsible.

I'm convinced–I don't want to have an open relay. How do I fix it?

Simply list in your rcpthosts file all the domains that your server is hosting (and for which it's acting as secondary mail exchanger, if any). Now you're safe.

But now my own customers get the message "Sorry, that domain isn't in my list of allowed rcpthosts." I'd like for my own customers to be able to use my server as a relay, but I can't possibly list every domain in my rcpthosts file to which they might want to send mail.

Nor should you try to! Fortunately, there's a way to get qmail-smtpd selectively to ignore the rcpthosts file. If the variable RELAYCLIENT is set in qmail-smtpd's environment, rcpthosts will be ignored and relaying will be allowed. What you need is a way to set RELAYCLIENT for your customers, but not for anyone else. (I'll refer to your users as "customers" here; substitute "employees," "students at my university," or whatever is appropriate in your case.)

First, you need a way to identify them. There's no sort of user name/password authentication in the SMTP protocol, so how do you identify whether a particular SMTP connection is from one of your customers? The surest way to distinguish a customer of yours from the rest of the world is by the fact that he's connecting to your server from a host on your network, i.e. a host with an IP address that's in your address space.

Once you know he's connecting from one of your IP addresses, you need a way to set RELAYCLIENT so that he can relay. It's pretty easy to set up qmail to do this. Read about selective relaying with tcpserver and qmail-smtpd to find out how.

Most of my customers aren't on my network–they use various ISPs. Can't I allow relaying if the mail is coming from one of my domains?

The way most people define "coming from one of my domains" is "has one of my domains in the sender address." The problem with this is that forging the sender address on a piece of mail is trivial, and you'd have to take the word of the sender that his address is what he says it is. There's clearly no security with this method.

Then how are they supposed to relay their mail?

The best thing for them to do is to use the SMTP servers provided by their ISPs. There's (usually) no reason that they should have to use your server to relay their mail; any server that'll agree to relay their mail will work, and ISPs' servers are there to relay their customers' mail.

Unfortunately, I've heard reports of a very small number of ISPs that require not only that the sending host be connected to the ISP's network, but also that the sender use the address provided by his ISP as his envelope sender address. I've never seen a non-Unix mail client that allows one to specify an envelope sender address that's different from the address that appears in the "From" header, so if your customer wants to relay mail through his ISP's SMTP server (and he has one of these envelope-checking ISPs) he won't be able to show in his "From" header the address that you've provided him–all his mail will have to appear to come from his ISP address.

So if my customer has one of these idiot ISPs and wants his mail to show an address with my domain, what is he to do?

There are some partial solutions to this problem; I don't think any of them is ideal. Probably the best is "SMTP-after-POP": you allow a particular IP address to relay through your server for a short period of time after a host at that address authenticates via POP. There are various implementations of SMTP-after-POP; one which doesn't require any patching is Bruce Guenter's relay-ctrl. The only problem with this approach is that at least some popular Windows mail clients are hard-wired to send any queued mail before checking mail. Your users will have to get into the habit of checking their mail before putting anything in their outboxes.

Another possible solution that people have recommended is running a separate instance of qmail-smtpd on a different IP address and a non-standard port, and telling your users to configure their mail clients to use it for their outgoing mail. One problem with this is that some mail clients don't allow you to set a non-standard SMTP port. Another problem is that it offers no real security, only "security through obscurity." You can make it somewhat safer, however, with tarpitting. This will help prevent it from being abused if it is discovered.

There are patches to qmail-smtpd that allow it to use SMTP AUTH, an extension to SMTP that implements user/password authentication for relaying. If your clients support SMTP AUTH, this is an excellent way to allow relaying to selected users who are not on your network. See the qmail web site for more information.

I think I've got everything set up correctly. How can I test my server to make sure it's not an open relay?

Try the relay tester at http://www.fabel.dk/relay/test/. Unlike many relay testers, this one requires that its probe message actually be relayed back to it in order for it to determine that you're an open relay. Other testers may flag you as an open relay if you simply accept a probe, whether or not you ultimately relay it.

Questions? Comments? I'm glad to hear them.

Chris Johnson
dcj-qmaildoc@palomine.net